Texas Bank Report

Texas Department of Banking, Charles Cooper, Commissioner October 2014

When times are hard it is easy to remember "the good old days."

Commissioner's Comments

Remember when? We like to remember "the good old days" when gas was cheap, you knew everyone in town, and life was simple. Of course, old times were probably never as good as we remembered. In fact, we revel in the difficulties of the past. How many times have you heard someone say "You don't know how good you have it now." We remember the best and the worst, and forget everything else in between. When times are hard it is easy to remember "the good old days."

The same is true in banking. We hear statements like "remember when a loan document was one page" or you just popped into your local bank for some friendly advice and a cup of coffee. We believe things were better in the past, and perhaps they were. Now, day in and day out we appear focused on the hardships and burdens of new regulations, credit, the economy, and thin interest margins. Because of these new pressures, bankers, customers, and regulators are on guard 24/7, ready for the next adversity we encounter.

But how often do we stop to think of the positives, the good? Banking today may not seem as wonderful as some of our memories; but, think about the technological advances in the last several years. Banking is on the cutting edge and light years faster than before. Transactions happen at the blink of an eye, and customers can access their information and accounts faster and more efficiently than ever. The efficiencies that have arisen because of improvements in procedures, and technology have given way to enhanced customer service and convenience.

The benefits are significant, but it should be noted that with any benefit, there can be a cost. Bankers and regulators have heard time and time again about the vulnerabilities associated with technology. Cyber threats, cybercrimes, cybersecurity – these are all key terms in today's banking world. The increased rate of cybercrimes has bankers and regulators working quickly, spending significant resources to protect their customer's data to ensure that cutting edge advances continue to be safe and trustworthy. Cybersecurity is an executive level issue that requires Board, CEO and Senior Executive, attention. It is no longer just a backroom challenge. The urgency to act is now because the frequency and seriousness of cyber threats is expanding rapidly.

The fact is the banking system today is a good deal more expansive than even ten years ago. A growing population, the internet and the need for everything to transact at a quicker pace has meant the system has not only grown but become much more complex. Operation and regulation of the banking industry are a complicated web of procedures and best practices, and legislation and regulations all designed hopefully to make the system safer and more stable.

As we reflect on progress, we are challenged to provide strong leadership to ensure our banking system enables each generation of Americans to make the claim that "*these* are the good old days."

Charles G. Cooper
Banking Commissioner

Communication Made Easier

The redesign of the agency's website in April features more information, easier navigation and improved accessibility. In addition, the new format gives the Department the ability to develop an official portal called Data Exchange (DEX) to communicate and share documents securely with entities regulated by the Department.

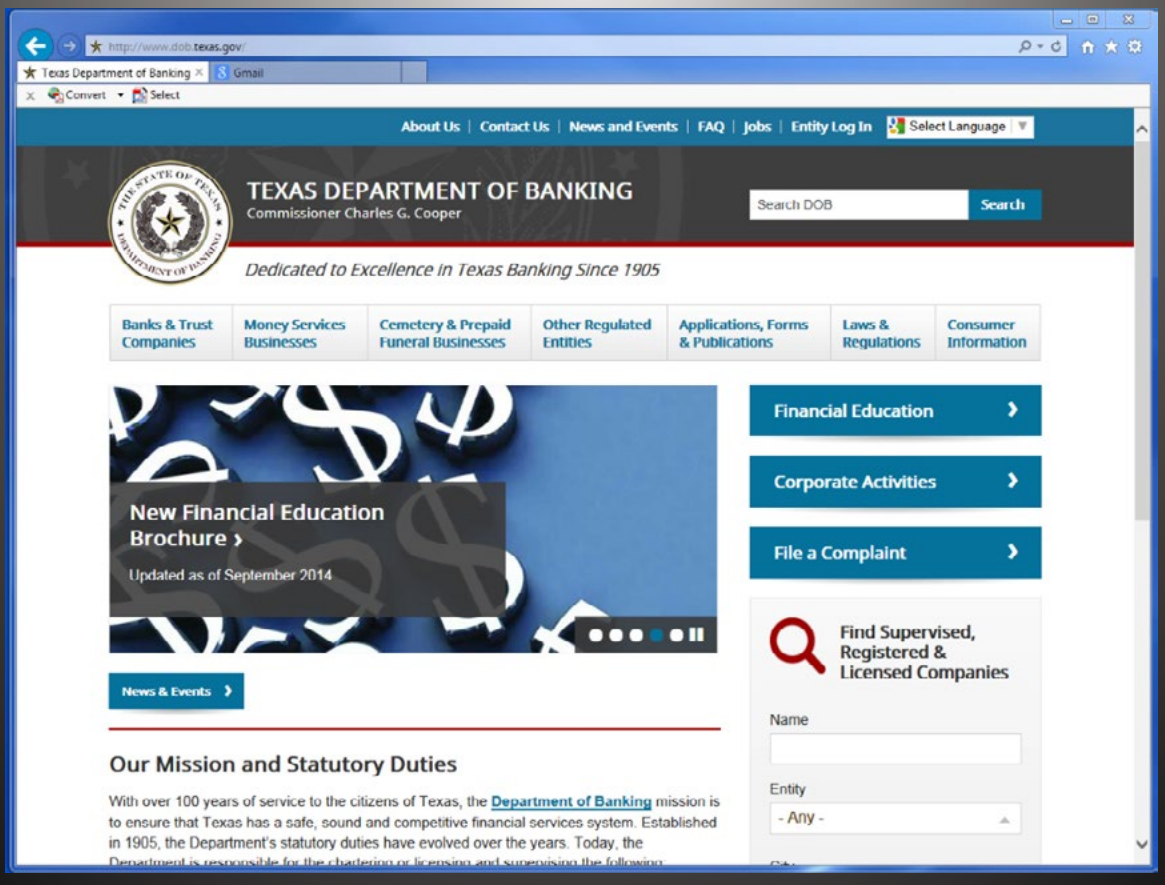
The portal is a secure vehicle that allows entities to upload material securely, providing integrity and confidentiality when needed to protect information being transmitted. A DEX user manual and tutorial video are available on the Department's website.

Key Features

- Securely upload examination request material
- Send and receive data files up to 100 MB
- Supports multiple file formats
- Allows for users to add comments for each file uploaded

Sign up today by contacting your ACES representative!

Click on Graphic Below to Play Video



Cybersecurity
Awareness is Key

By Linda Pearson

Cybersecurity awareness is the most important tool in preventing your customers and employees from becoming cybercrime victims. In fact, it is so important that the President issued a nationwide proclamation officially designating October as "National Cybersecurity Awareness Month." The United States Department of Homeland Security and the National Cyber Security Alliance developed a program to alert the public and provide access to information and resources. If you missed the opportunity to participate in the October 2014 activities, it is never too late to start raising cybersecurity awareness in your organization and community. You do not want to wait until you or one of your customers becomes a victim to realize the importance of cybersecurity.

"It can't happen to us" is a phrase bank examiners frequently hear from bankers. The "us" refers to both the bank and the bank's customers. Unfortunately, that statement is not true. Cybercriminals are targeting smaller institutions and consumers. Account takeover was once thought to only happen to corporate customers because they can hold large account balances. A few years ago, larger banks started seeing retail customers become account takeover targets, which is now spreading rapidly to retail customers in the community banks.

A considerable amount of information and resources are available on the Internet to assist in creating awareness programs for bank employees and customers. This information can be helpful and over-

whelming at the same time, but raising cybersecurity awareness is a crucial part of an effective information security program. Two noteworthy resource websites are Homeland Security and National Cyber Security Alliance.

Choosing a specific area to focus on, such as strengthening passwords, patching and updating computers and mobile devices, and signs of compromise, is a good starting place to develop an awareness program. Topics can be reviewed frequently as new ways to reinforce mitigation strategies are constantly evolving. For instance, the concept of strong password controls has been around since long before the concept of "cybercrime" became a buzzword. The new twist to stronger passwords is to have a different password for each of your accounts. Using different passwords today requires a mechanism to manage the multitude of passwords in a secure manner. However, signals about a password compromise change frequently as cybercriminals undoubtedly adapt to stronger controls. Password management is a developing technology with better user interfaces and more secure solutions becoming available constantly.

An important next step is to select the method(s) for educating customers and employees. The message needs to be clear and easy to understand from the technology challenged to the early adopters. Customer awareness programs can be as simple as banners on a bank's website and online banking messages or as involved as hosting community outreach programs. The fundamental concept is to keep the messages accessible to customers so that thinking securely becomes an automatic, recurring thought process.

Most banks use online education programs to raise awareness among employees. While these programs provide a good starting point for raising employee awareness, it is usually not enough. These third-party programs are generic and should be supplemented with specific information about threats and vulnerabilities unique to your institution as identified during the risk assessment process. For example, a branch staff meeting could cover a different risk every month that affects that particular location.

After your program has been around for a while, you should gauge the effectiveness of the message you are delivering. When cybercriminal compromises become less frequent and customers rarely call the bank wondering what happened to their money, you will know you have succeeded in raising awareness.

For questions regarding this and other IT security issues, contact our Chief IT Security Examiner, Linda Pearson or the Director of IT Security Examinations, Phillip Hinkle.

Responding to Subpoenas
For Bank Records - A Primer

By Catherine Reyer

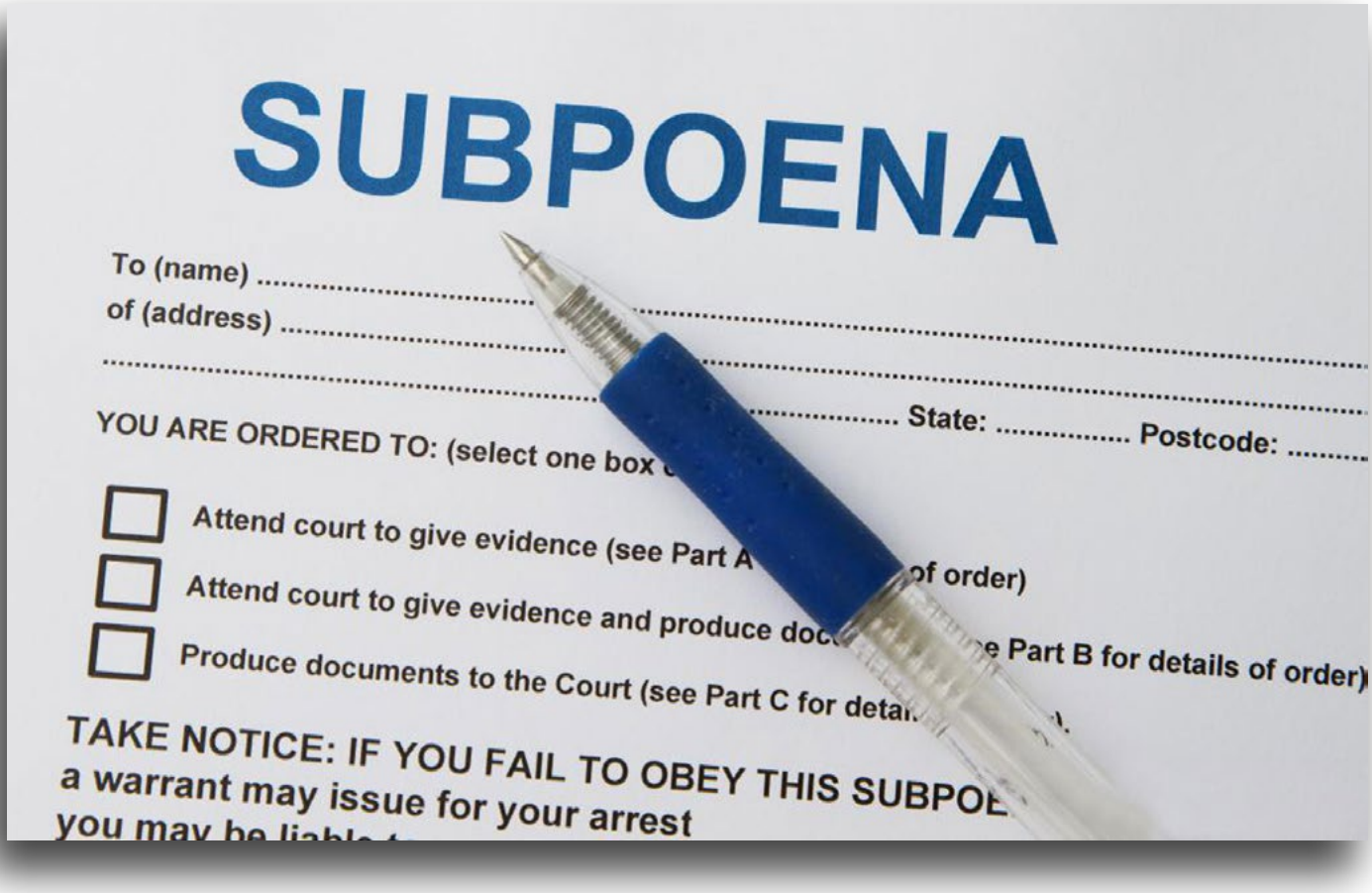
You have just received a subpoena for bank records. What now? Just the word "subpoena" itself is a little scary. It comes from the Latin *sub* (under) and *poena* (penalty). Literally, the entity receiving the subpoena (although not a party to the underlying legal proceeding) is required to produce something "under penalty" of the issuing court. All subpoenas contain a deadline by which the recipient must provide some kind of response.

First, it is helpful to understand the different types of subpoenas. Careful review of the document will show the jurisdiction of the issuing court, i.e. state or federal. It will also identify whether the matter is a civil or criminal proceeding. It will further specify whether it is a *subpoena duces tecum*, (bring with you), meaning that it requires the recipients to produce documents; or if it is a *subpoena ad testificandum,* meaning that live testimony is required. Finally, a subpoena may be issued along with an order signed by the judge of the issuing court, or it may be issued directly by an attorney representing one of the parties in the case. Once you have identified the court in which the proceeding lies, it may be beneficial to develop at least a basic understanding of the case by reviewing the pleadings in PACER (for federal cases) or by contacting the clerk of the particular state district court. This understanding may frame how you prepare your response.

Once you have identified the court, type of case, and general nature of the subpoena, the next step is to review carefully the description of documents or testimony being sought. Of primary concern is whether the responsive material is subject to state or federal confidentiality provisions. For example, if it includes reports or responses from regulators concerning the institution's financial condition or business affairs, it may be unlawful to provide the information. In particular, the Texas Department of Banking (Department) considers reports of examination, related progress reports, memorandums of understanding, and consent orders to be confidential under provisions of the Government Code or the Finance Code.

Title 7, Section 3.111(b)(2) of the Texas Administrative Code defines confidential information broadly:

> Written and oral information obtained directly or indirectly by the department relative to the financial condition or business affairs of a financial institution, or a present, former, or prospective



shareholder, participant, officer, director, manager, affiliate, or service provider of a financial institution, whether obtained through application, examination, or otherwise, and all related files and records of the department, regardless of the form of the information when obtained or as held by the department or when the department first obtained it, and whether or not the information is part of the department's official files or records.

The rule goes on to prohibit disclosure of confidential information with certain limited exceptions, and provides a process for responding to subpoenas:

1. **Promptly notify the Department of the request**. This is crucial. Although the burden of providing the response rests squarely on the bank that has received the subpoena, the Department will need time to review the request and determine for itself whether and how to respond. Many factors may affect how long it will take to formulate the response, such as questions about relevance and confidentiality. Longer lead time for handling is especially important if a response must be reviewed and coordinated among multiple parties, such as federal regulators, who may also have an interest in protecting the information.

2. **Provide the Department with a copy of the subpoena and the requested documents.** Again, prompt submission to the Department is key given the elements above. This is particularly true if the requested information is voluminous, as the Department will need time to review and determine whether an independent response is required.

3. **File and obtain a ruling on a motion for a protective order and in-camera inspection**. The motion will need to be filed in the court where the underlying proceeding lies before the deadline for responding to the subpoena. The protective order will set limits on who may view the responsive information and specifies certain conditions on disclosure. An in-camera inspection requires that only the judge assigned to the case may review the confidential documents.

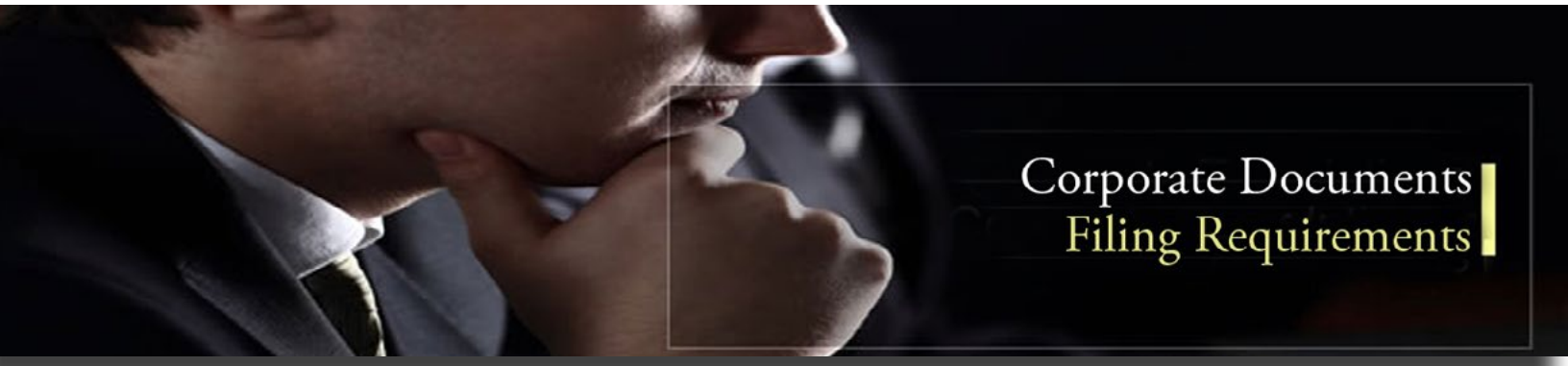
If you receive a subpoena and have questions about applicable laws and rules, you may contact the Department's General Counsel Catherine Reyer at 512-475-1327.

Filing

For Certa

The mission of the Corporate Division is to process filings and maintain official corporate records for the Department in a timely, effective and accurate manner, while ensuring statutory requirements are met. The types of filings processed by Corporate have evolved over the years both in terms of the expanded range of entities submitting filings and the complexity of the filings themselves.

Many types of activities or actions undertaken by a state bank, state bank holding company or a trust company require either a notice or application to be filed with the Department. While the need to submit certain types of filings such as branch or merger applications are self-explanatory, the necessity to submit other filings may not be as clear. The Corporate Division has put together a list of trouble spots below where the necessary filing or information is either not provided to the Department or is inadvertently omitted from a particular filing.



Address Changes without a Move

If the physical address changes for a home office or a branch of a Texas state bank or trust company without a move, a notice letter can be provided by mail, fax, or email. The notice should include an explanation as to why the physical address has changed and a confirmation that relocation did not take place. The exact street address and the effective date of the change must also be provided.

Contact or Mailing Address Changes

If a Texas state bank or trust company changes their mailing address, zip code, email, website address, area code, telephone, fax, or suite number, an email providing the changes should be submitted to update the Department's database.

Loan Production Office (LPO) and/or Deposit Production Office (DPO)

If a state bank plans to establish a LPO and/or DPO, the bank must submit a notice letter to the Department for each LPO and/or DPO location at least 31 days before the establishment of the office. Instructions can be found on the Department's website under Applications & Forms.

If an out-of-state financial institution plans to establish a LPO or DPO in Texas, no application or notice to the Department is required. However, it must file an application

g and Notification Requirements

ain Types of Corporate Related Transactions

By Clara Zamarripa

for registration with the Secretary of State before operating a LPO or DPO in Texas pursuant to Texas Finance Code §201.102.

If a state bank plans to relocate or close an existing LPO or DPO in Texas, the bank must provide a notice letter before the fifth day preceding the date of relocation or closure by mail, fax, or email. The written notification must include the physical address of the LPO or DPO to be relocated or closed, and the date of the relocation or closure.

Sublease of Office Space

If a state bank or trust company would like to sublease office space to an affiliated entity, prior approval from the banking commissioner is only required if the transaction cannot be approved by at least a majority of a quorum composed entirely of disinterested directors of the board.

Subsidiaries

If any information changes for a state bank's subsidiary, a notice letter must be provided to the Department by mail, fax, or email. The notice should include the name and address of the subsidiary, the change to be made to the subsidiary, and the effective date of the change. Such changes may include the "active or inactive" status, closure, and name or address change.

Change of Control of a State Bank, State Bank Holding Company, or Trust Company

An application must be filed if a person or entity, directly or indirectly, acquires a legal or beneficial interest in voting securities of a state bank, state bank holding company, or trust company, or a corporation or other entity owning voting securities of a state bank, state bank holding company, or trust company if, after acquisition, the person or entity would control the state bank, state bank holding company, or trust company.

In certain circumstances, a notice filing may be submitted in lieu of an application, such as in the passing of a significant shareholder. A list and description of exceptions can be found in Section 33.005 of the Texas Finance Code and 7 Texas Administrative Code §15.81.

Mergers

For any merger application where the surviving financial institution will be a state financial institution, a restated Certificate of Formation must be incorporated with the Certificate of Merger pursuant to 7 Texas Administrative Code §15.104(b).

Should you have questions or need assistance with application or notice filing requirements, please contact the Corporate Activities Division at (512) 475-1322 or by email.

Promoting a Culture of Compliance

By Dianne Dennis

The Financial Crimes Enforcement Network (FinCEN) issued Advisory FIN-2014-A007 in August 2014, to financial institutions highlighting the importance of developing a strong Bank Secrecy Act and Anti-Money Laundering (BSA/AML) culture of compliance within the organization regardless of size or industry. The Advisory was released in response to AML enforcement actions that confirm the culture of an organization is critical to its compliance. While the Advisory does not change any existing expectations or obligations under BSA/AML requirements, it does outline six areas that can strengthen a financial institution's BSA/AML compliance culture.

1. **Leadership Should Be Engaged**

   A strong compliance culture begins at the top. The board and senior management are not only responsible for the institution's compliance with BSA, but should also be visible within the organization in order to create a "culture of compliance." Leaders should receive periodic training that is tailored to their responsibilities and have an appropriate understanding of the institution's BSA/AML obligations in order to effectively allocate resources to the BSA/AML compliance function.

2. **Compliance Should Not Be Compromised By Revenue Interests**

   The governance structure of a financial institution should be one that ensures the BSA/AML compliance staff has sufficient authority, resources, and autonomy to effectively manage and mitigate risk within the organization and file all necessary reports. As an example, the Advisory uses a Money Service Business (MSB) that derives a significant percentage of their revenue from the activity of their agents. FinCEN states that inappropriate activity by an agent of an MSB should be thoroughly investigated and appropriate action should be taken, including possible termination of the account.

3. **Information Should Be Shared Throughout the Organization**

   The Advisory encourages organizations to share information across all various departments with the compliance staff. Recent enforcement actions show that several institutions had relevant information in their possession but failed to make it available to BSA/AML compliance staff. According to FinCEN this may have been due to a lack of a mechanism for sharing information, lack of understanding as to why the information is important, or an intentional decision to prevent the compliance staff from having access to the information.

4. **Leadership Should Provide Adequate Human and Technological Resources**

   The board must designate an individual responsible for coordinating and monitoring the day-to-day BSA/AML compliance function. This individual should be knowledgeable in BSA and have sufficient authority and resources to administer the program. Institutions with higher risk profiles and substantially higher volumes of activity may need to use automated systems for identifying and monitoring suspicious activity. Failure to provide adequate staffing may lead to alerts not being reasonably designed to capture the institution's risk, being inappropriately dismissed, or creating a backlog of alerts that may result in untimely reporting of suspicious activity.

5. **The Program Should Be Effective and Tested By an Independent and Competent Party**

   Compliance programs should be commensurate with the

bank's risk profile and include ongoing risk assessments, sound risk-based customer due diligence procedures, and appropriate detection and reporting of suspicious activity. The compliance program should be periodically tested and leaders should ensure the party testing the program (whether internal or external) is independent, qualified, unbiased, and does not have conflicting business interests in the outcome of the compliance test program. An independent test of the program by qualified individuals enables the institution to identify deficiencies and take appropriate action.

6. Leadership and Staff should Understand How Their BSA Reports Are Used

Leadership and staff at all financial institutions should understand the purpose of BSA reports and how the information is used. The reports filed by institutions serve as tips to initiate investigations, expand existing investigations, promote international information exchange, and identify significant relationships, trends, and patterns. Understanding and communicating the context and the purpose of FinCEN's BSA/AML regulations is important and institutions are urged to consider including this information as part of their ongoing training requirements.

"Based on the enforcement cases I have seen time and time again, both during my time as a prosecutor at the U.S. Department of Justice and now as Director of FinCEN, I can say without a doubt that a strong culture of compliance could have made all the difference. If I were to find myself responsible for BSA/AML compliance within any financial institution, my first order of business would be to pay attention to these core, fundamental concepts. Because once you have a strong culture in place, including support of your institution's leadership, you have a firm foundation on which to build an effective program."

– FinCEN Director Jennifer Shasky Calvery

First State Bank of Uvalde's Financial Literacy Efforts Means Thinking Outside the Box

By Leilani Lim-Villegas

The Department continues to identify Who's Who in financial education in Texas by conducting ongoing statewide visits with bank Chief Executive Officers and Presidents. In April 2014, a visit was scheduled with First State Bank of Uvalde (FSB) to discuss their financial education efforts. As part of any meeting, financial literacy kits with the curricula are provided, the financial needs of their communities are discussed, the bank's target customers are identified, and a list of resources are provided to motivate state-chartered banks to jumpstart or improve their financial literacy efforts. Senior Vice President, William Dillard was the contact for the bank's program. As the meeting proceeded, he provided a thick white binder of documentation of the community outreach programs FSB has been involved with during the past two years. The information was well-organized with press releases, newsletter articles, and photographs of their community events. It was apparent the bank is passionate about financial education and for this, the Texas Department of Banking is pleased to highlight FSB as the Financial Education Spotlight for this edition of the Texas Bank Report. This is their story.

In February 2012, FSB Chairman and CEO, Dickie Geries asked William Dillard to begin developing a financial literacy program. At the time, the bank's efforts were limited to providing occasional assistance to area school teachers upon request. In most cases this meant sending teachers bank-related literature or check practice kits. Looking deeper into the resources available, Mr. Dillard made a point to name a few key organizations and individuals that were ready and willing to assist. Among those key resources were the Texas Bankers Association (TBA), the Independent Bankers Association of Texas (IBAT), the Texas Department of Banking, and the Federal Reserve Bank of Dallas.

Mr. Dillard's assistant, Ms. Mary Nicole Horn deserves recognition for initiating the bank's financial literacy program. A former classroom teacher herself, Nicole was a natural fit in working with area schools and did the heavy lifting early on to help get the program off the ground. In August 2013, Ms. Vennessa McLerran joined FSB as a Marketing Assistant and Financial Literacy Specialist and since that time has been the point person on most elements of the current program. She has been instrumental in developing custom-tailored curriculums to meet the needs of the students and parents. Her bilingual skills have also been instrumental in assisting some of the students with an understanding of money managing concepts.

Partnerships Assist Outreach

In 2013, the FSB program took a substantially different direction. Although the bank was meeting the needs of school-aged young people, there was a need to think outside the box and develop new strategies to address the money management needs of older students and family units. The initiative could not have been successful without the help of groups and organizations who were already serving the needs of people in their own various and unique ways. As such, partnerships began forming with some established area programs. These organizations continued to provide their clients with the same services they had provided all along, and FSB joined them to provide financial literacy training. This team effort was very effective and the bank gained a foothold into the underserved groups, while communities benefitted from the bank's expertise in money management. The bank currently partners with five organizations: VITA, AVANCE, Wintergarden District Boy Scouts, St. Henry D'Osso Family Literacy Project, and Dia de Los Niños; with the goal of increasing partnerships to better serve the financial education needs of more individuals.

Financial Literacy Requirement for Scholarship

Recently, FSB signed a historic agreement with Sul Ross State University Rio Grande College to provide a unique $1,000 per semester scholarship. In addition to the usual list of requirements, full-time student status and a minimum grade point average of 3.0, students who apply for the scholarship are required to attend a six-week financial literacy course taught by bank employees. FSB has learned that they are the first financial institution to directly tie financial literacy to a scholarship. This program is a natural fit for the college, which has developed an initiative to assist students who wish to obtain a four-year degree with minimal student loan debt.

As a result of the bank's community and financial literacy efforts, FSB has been recognized by the Texas Bankers Foundation and the IBAT Education Foundation. In 2014, they were awarded the Texas Bankers Foundation LiFE Award. Congratulations to First State Bank of Uvalde for a job well done and we wish them continued success!

For more information on financial education visit the Texas Department of Banking's financial education section of the website or contact the Financial Education Coordinator.

Senior Vice President, Bill Dillard, introduces the partnership to parents of St. Henry De Osso Family Project to provide financial literacy sessions with Federal Reserve Bank of Dallas's "Building Wealth" program. September 5, 2013.

The junior and senior classes of Knippa High School in Knippa, Texas, get an introduction to Federal Reserve Bank of Dallas's "Building Wealth" program given by Senior Vice President, Bill Dillard and FSB's Vennessa K. McLerran. March 2014.

Guadalupe Ruiz and family receive a Financial Literacy Certificate of Achievement Award for completing FSB's "Building Wealth" sessions at AVANCE in Uvalde, Texas. April 2014.

TABLE I
Quarterly Balance Sheet and Operating Performance Ratios
for Texas State-Chartered Banks 6/30/14 Through 6/30/13

ACCOUNT DESCRIPTIONS (IN MILLIONS OF $)	6/30/14	3/31/14	12/31/13	9/30/13	6/30/13
Number of State-Chartered Banks	274	280	283	283	288
Total Assets of State-Chartered Banks	225,509	220,567	216,541	208,785	203,295
Number of Out-of-State, State-Chartered Banks Operating in Texas	26	26	26	27	29
Total Texas Assets of Out-of-State, State-Chartered Banks Operating in Texas	43,337	43,337	43,337	43,572	40,210
Subtotal	268,846	263,904	259,878	252,357	243,505
Less: Out-of-State Branch Assets/Deposits	-44,618	-44,618	-44,618	-44,618	-42,210
**Total State Banks Operating in Texas	224,228	219,286	215,260	207,739	201,295
BALANCE SHEET (Tx. State-Chartered Banks)					
Interest-Bearing Balances	14,249	17,563	17,102	17,154	12,526
Federal Funds Sold	791	966	918	920	1,174
Trading Accounts	436	347	362	341	375
Securities Held-To-Maturity	15,750	15,275	14,944	14,403	14,381
Securities Available-for-Sale	43,057	42,155	41,898	41,111	41,338
Total Securities	58,807	57,430	56,842	55,514	56,094
Total Loans	132,167	125,727	122,872	117,212	116,921
Total Earning Assets	206,014	201,686	197,734	190,800	186,715
Premises and Fixed Assets	3,650	3,600	3,579	3,428	3,344
Total Assets	225,509	220,567	216,541	208,785	203,295
Demand Deposits	25,735	25,102	25,282	23,202	21,355
MMDAs	100,364	97,756	94,935	90,913	88,429
Other Savings Deposits	16,417	16,018	15,623	14,806	14,325
Total Time Deposits	35,750	35,623	35,690	35,232	34,821
Brokered Deposits	2,361	2,000	1,924	1,785	1,710
Total Deposits	187,798	184,274	181,010	172,990	167,411
Federal Funds Purchased	3,132	3,155	3,396	3,269	3,338
Other Borrowed Funds	5,192	4,652	4,556	5,677	5,796
Total Liabilities	200,165	196,025	192,760	185,953	180,710
Total Equity Capital	25,765	24,543	23,780	22,833	22,585
Loan Valuation Reserves	1,606	1,608	1,600	1,580	1,575
Total Primary Capital	27,371	26,151	25,380	24,413	24,160
Past Due Loans > 90 Days	221	306	335	361	356
Total Nonaccrual Loans	890	927	1,062	1,187	1,249
Total Other Real Estate	545	575	603	614	564
Total Charge-Offs	143	69	378	276	190
Total Recoveries	75	38	153	103	68
Net Charge-Offs	68	31	225	173	122
INCOME STATEMENT					
Total Interest Income	3,619	1,776	6,838	5,007	3,315
Total Interest Expense	267	135	586	442	302
Net Interest Income	3,352	1,641	6,252	4,565	3,013
Total Noninterest Income	1,424	682	2,879	2,179	1,458
Loan Provisions	81	38	235	179	120
Salary and Employee Benefits	1,730	850	3,403	2,528	1,684
Premises and Fixed Assets Expenses (Net)	397	198	758	557	368
All Other Noninterest Expenses	975	479	1,909	1,353	920
Total Overhead Expenses	3,102	1,527	6,070	4,438	2,972
Securities Gains (Losses)	22	17	53	45	42
Net Extraordinary Items	0	0	0	0	0
Net Income	1,211	582	2,203	1,659	1,085
Cash Dividends	572	266	1,266	872	605
RATIO ANALYSIS					
Loan/Deposit	70.38%	68.23%	67.88%	67.76%	69.84%
Securities/Total Assets	26.08%	26.04%	26.25%	26.59%	27.59%
Total Loans/Total Assets	58.61%	57.00%	56.74%	56.14%	57.51%
Loan Provisions/Total Loans	0.12%	0.12%	0.19%	0.20%	0.21%
LVR/Total Loans	1.22%	1.28%	1.30%	1.35%	1.35%
Net Charge-Offs/Total Loans	0.05%	0.02%	0.18%	0.15%	0.10%
Nonperforming+ORE/Total Assets	0.73%	0.82%	0.92%	1.04%	1.07%
Nonperforming+ORE/Primary Capital	6.05%	6.91%	7.88%	8.86%	8.98%
Net Interest Margin	3.25%	3.25%	3.16%	3.18%	3.23%
Gross Yield	4.47%	4.46%	4.49%	4.58%	4.70%
Return on Assets	1.07%	1.06%	1.02%	1.06%	1.07%
Return on Equity	9.40%	9.49%	9.26%	9.66%	9.61%
Overhead Exp/TA	2.75%	2.77%	2.80%	2.83%	2.92%
Equity/Total Assets	11.43%	11.13%	10.98%	10.94%	11.11%
Primary Capital/Total Assets+LVR	12.05%	11.77%	11.63%	11.61%	11.79%

*Unrealized gains/losses are already included in equity capital figures.
**Total State Banks Operating in Texas includes branches of out-of-state, state-chartered banks.
Data was derived from the FDIC website.

TABLE II
Comparative Statement of Condition
Commerical Banks Domiciled in Texas
June 30, 2014 and June 30, 2013

ACCOUNT DESCRIPTIONS (In Millions of $)	6/30/2014 STATE CHARTERED		6/30/2014 NATIONAL CHARTERED		6/30/2014 ALL BANKS		6/30/2013 ALL BANKS	
Number of banks	274	% TA	206	% TA	480	% TA	512	% TA
BALANCE SHEET								
Interest-Bearing Balances	14,249	6.3%	7,562	5.3%	21,811	5.9%	21,171	5.9%
Federal Funds Sold	791	0.4%	17,569	12.4%	18,360	5.0%	16,958	4.8%
Trading Accounts	436	0.2%	36	0.0%	472	0.1%	410	0.1%
Securities Held-To-Maturity	15,750	7.0%	3,064	2.2%	18,814	5.1%	17,134	4.8%
Securities Available-For-Sale	43,057	19.1%	20,833	14.7%	63,890	17.4%	64,234	18.0%
Total Securities	58,807	26.1%	23,933	16.9%	82,740	22.5%	81,778	23.0%
Total Loans	132,167	58.6%	85,012	59.9%	217,179	59.1%	211,416	59.3%
Total Earning Assets	206,014	91.4%	134,076	94.4%	340,090	92.5%	331,323	93.0%
Premises & Equipment	3,650	1.6%	1,753	1.2%	5,403	1.5%	5,338	1.5%
TOTAL ASSETS	225,509	100.0%	142,030	100.0%	367,539	100.0%	356,297	100.0%
Demand Deposits	25,735	11.4%	15,491	10.9%	41,226	11.2%	36,089	10.1%
MMDAs	100,364	44.5%	48,634	34.2%	148,998	40.5%	137,654	38.6%
Other Savings Deposits	16,417	7.3%	31,524	22.2%	47,941	13.0%	51,094	14.3%
Total Time Deposits	35,750	15.9%	18,673	13.1%	54,423	14.8%	56,958	16.0%
Brokered Deposits	2,361	1.0%	3,779	2.7%	6,140	1.7%	4,189	1.2%
Total Deposits	187,798	83.3%	120,891	85.1%	308,689	84.0%	296,638	83.3%
Fed Funds Purchased	3,132	1.4%	1,250	0.9%	4,382	1.2%	4,763	1.3%
Other Borrowed Funds	5,192	2.3%	2,686	1.9%	7,878	2.1%	11,140	3.1%
TOTAL LIABILITIES	200,165	88.8%	125,944	88.7%	326,109	88.7%	317,811	89.2%
Equity Capital	25,765	11.4%	16,086	11.3%	41,851	11.4%	38,486	10.8%
Allowance for Loan/Lease Losses	1,606	0.7%	1,261	0.9%	2,867	0.8%	3,160	0.9%
Total Primary Capital	27,371	12.1%	17,347	12.2%	44,718	12.2%	41,646	11.7%
Past due >90 Days	221		263		484		717	
Nonaccrual	890		827		1,717		2,626	
Total Other Real Estate	545		155		700		1,048	
Total Charge-Offs	143		77		220		350	
Total Recoveries	75		33		108		114	
INCOME STATEMENT	Y-T-D		Y-T-D		Y-T-D		Y-T-D	
Total Interest Income	3,619	100.0%	2,270	100.0%	5,889	100.0%	5,842	100.0%
Total Interest Expense	267	7.4%	150	6.6%	417	7.1%	510	8.7%
Net Interest Income	3,352	92.6%	2,120	93.4%	5,472	92.9%	5,332	91.3%
Total Noninterest Income	1,424	39.3%	755	33.3%	2,179	37.0%	2,274	38.9%
Loan Provisions	81	2.2%	(34)	-1.5%	47	0.8%	137	2.3%
Salary & Employee Benefits	1,730	47.8%	959	42.2%	2,689	45.7%	2,662	45.6%
Premises & Fixed Assets (Net)	397	11.0%	216	9.5%	613	10.4%	603	10.3%
All Other Noninterest Expenses	975	26.9%	614	27.0%	1,589	27.0%	1,552	26.6%
Total Overhead Expenses	3,102	85.7%	1,789	78.8%	4,891	83.1%	4,817	82.5%
Securities Gains(losses)	22	0.6%	5	0.2%	27	0.5%	61	1.0%
Net Extraordinary Items	0	0.0%	1	0.0%	1	0.0%	1	0.0%
NET INCOME	1,211	33.5%	841	37.0%	2,052	34.8%	2,040	34.9%
Cash Dividends	572		416		988		1,062	
Average ROA	1.07%		1.18%		1.12%		1.15%	
Average ROE	9.40%		10.46%		9.81%		10.60%	
Average TA ($ Millions)	823		689		766		696	
Average Leverage	11.43%		11.33%		11.39%		10.80%	
Dividends/Net Income	47.23%		49.46%		48.15%		52.06%	

*Unrealized gains/losses are already included in equity capital figures.
Table includes only banks domiciled in Texas. Branches of out-of-state banks are not included.
Data was derived from the FDIC website.